UTM（統合脅威管理）

UTM100

UTM100Std S / UTM100Std M / UTM100Std L
UTM100Pro S / UTM100Pro M / UTM100Pro L

世界最高水準のハイクオリティUTM

ウイルス対策ソフトだけでは阻止できない脅威

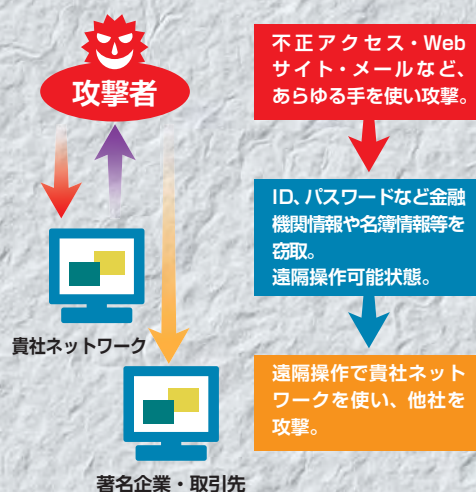
拡大するネット不正送金被害・データ流出のニュースが絶えずヘッドラインを賑わしています。
なかでも近年のサイバー犯罪の主な目的は、金銭を窃取することです。
今やネットワークセキュリティは必須の課題であり、企業では効果的な対策を実施することが重要です。

狙われる企業ネットワーク

金銭搾取を目的としたサイバー犯罪は年々巧妙になっています。
企業の大小に係わらずセキュリティの甘い企業がターゲットにされています。

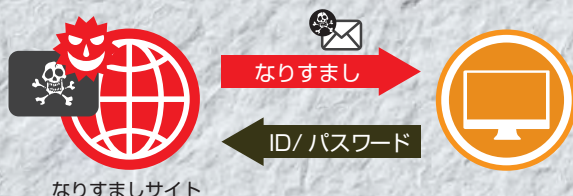
違法サイトの閲覧や不明なメールアドレスの閲覧をしないというだけでは、サイバー犯罪を防ぐことは出来ません。
近年のサイバー攻撃は、既知の著名サイト、既知のメールアドレスを経由してやってきます。

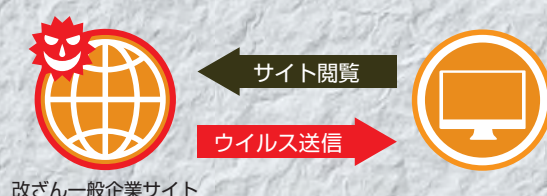
まずセキュリティの甘い企業に侵入。
ID、パスワードなどの金融機関情報や名簿情報など換金できる情報を抜き去った後に、よりセキュリティの高い企業へ侵入するための踏み台とされます。

世界では１日約６万ものウイルスが発見されています。

多様化・巧妙化するサイバー犯罪の手口

データの重要性・価値が高まっていますが、それを狙う手口も進化しています。
サイバー犯罪の特異な点は、感染した企業は単に被害者になるだけでなく取引先等に新たにウイルスを発信する・著名企業や官公庁を襲う加害者になり得ることです。被害は自社の業務支障だけでなく、他社からの信用失墜など拡大していきます。
また、不正送金先や情報漏えい先は、国内の捜査権の及ばない第３国がほとんどで、サイバー攻撃者までたどるのは極めて困難な状況です。

なりすまし（フィッシング）

金融機関・オンラインショッピング・オークションサイト等を騙った「なりすましメール」を送信し、偽サイトへ誘導して銀行口座情報・クレジットカード情報を窃取します。

Web サイト改ざん

官公庁や企業の Web サイトを見ただけでウイルスに感染するケースが急増しています。これまで遠隔操作型ウイルスやネットバンキングの口座情報やクレジットカード情報を盗み出すウイルスが発見されています。

自己増殖

ウイルスは感染した PC のメールソフトからアドレス帳を読取り、登録されているメールアドレスにウイルスを添付して送信します。また社内 LAN の共有フォルダや USB メモリなどのデバイスに自己増殖を行います。

不正アクセス

直接 LAN に侵入する不正アクセスは無差別に行われていて、セキュリティの甘い企業が狙われています。
侵入した攻撃者は PC をボット化し（自在に遠隔操作できるようにする）、情報を抜き、著名企業攻撃の踏み台にします。

UTM100は安全で快適なネットワークを提供します

個人のインターネット利用と違って企業でのインターネット利用は、
●ネットバンキングでの取扱金額の大きさ●個人情報の取扱い
●利用人数●メールの利用頻度●取引先との信用問題
などにより、一度被害を受けるとその影響は莫大なものになります。

企業でのインターネット利用のウィークポイント

企業でのネット利用には、以下の様な特長があります。セキュリティ対策を怠っていると、膨大な被害に繋がります。

■ 従業員のネット利用内容を把握できない

有害サイトへの接続や危険な P2Pソフトの利用を事前に報告する従業員はいません。
アンダーグランドソフトの入手を試みる従業員の中にはアンチウイルスソフトを無効にして利用する人もいます。

UTM100 は、有害サイトや業務に関係のないサイトへの接続、P2P ソフトの利用を制御し、一元管理できます。

■ 常に常時接続している

家庭と違い、企業にはサーバー・複合機・T V会議システムなど 24 時間起動している機器が多く存在します。
ネットへの接続時間が長いと不正アタックの危険性が高まります。

UTM100 は、お客様のネットワーク自体への不正侵入をブロックします。

■ 個人情報が多い（B to C 企業の場合）

B to C（Business to Consumer/ 個人対象ビジネス）企業では、個人情報を多く取り扱っています。個人情報は、名簿として換金できることからサイバー攻撃者から狙われやすく、また情報漏えいが発生した場合には個人情報保護法により情報漏えいで被害にありながら、逆に罰則の可能性もあります。

UTM100 は、有害サイトへの通信による情報漏えいをブロックします。

■ メールチェックを迅速に行う必要がある

メールによるビジネス連絡が主流となっている現在、SPAM（スパム）メールと呼ばれる迷惑メールも大量に送られてきています。SPAM メールが混在することにより、大切なメールを見逃してしまう可能性が増え、その選別などにかかる労力は本来ビジネスを迅速・確実に行うためのメールがビジネスを鈍化させてしまいます。

UTM100 は、パソコンに負荷をかけずに SPAM メールをブロックします。

■ 運用資金が多い

オンラインバンキングが日常化し、その取引金額も大きくなってきている反面、金融機関ではなりすましメール等による口座情報流失による被害に対して「補償減額または補償せず」という発表をしています。

一般社団法人全国銀行協会 2014 年7月

UTM100 は、SPAM メールブロック・有害サイト接続ブロックにより二重になりすましから保護します。

対処をしないと大きく拡大するネットワーク被害

被害は一次的なものではなく、対処を行わないと大きく拡大します。ウイルス感染や情報漏えい被害は一次的被害だけでなく二次被害を引き起こします。感染したパソコンは社内ネットワークに接続している他のパソコンやメールアドレス等を元に取引先へも感染を広げます。

一度被害に合うとそれは、自社の業務支障だけでなく、取引先からの信用失墜などに拡大していきます。

UTM100の主な特長

攻撃者は、検出を避けるために、その攻撃方法を絶えず変更しています。
UTM100は､130万以上のウイルス情報と1日最大4万件更新している有害サイトのURL情報によって、新たに出現するこれらの脅威からお客様のネットワークを保護します。

優れた防御力

- ウイルスパターン数　130万種以上
- URLフィルタリング　109カテゴリ・3,500万アドレス

膨大な脅威データと豊富な経験を基盤としたUTM100は、業界最多のウイルスデータベース・有害サイト情報を保持し、過去のものから最新のものまで、様々なウイルスからお客様のネットワーク環境を保護します。

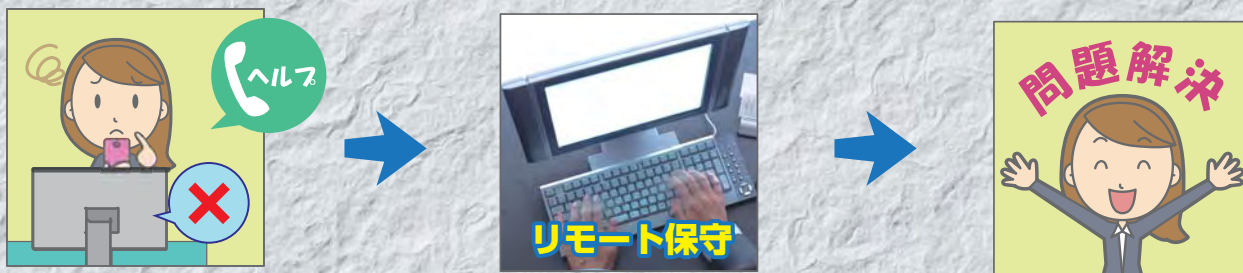
必要とする次世代ファイアウォールの機能を搭載

従来型ファイアウォールは、通信データ（パケット）のヘッダ情報（送信元 / 宛先 IP アドレスとポート番号）を検査して、その通信を許可するかどうかを判断します。このファイアウォールを突破するため、他のソフトが使用しているポート番号を利用するソフトがあります。そのような通信も制御できるのが「次世代ファイアウォール」です。

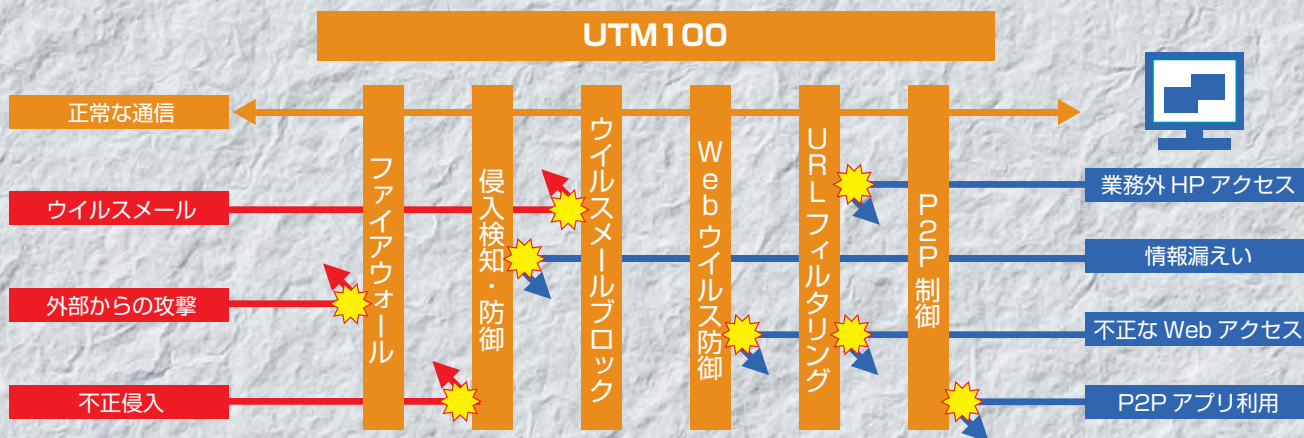
優れたユーザービリティ

簡単な管理と詳細なレポート作成機能により､複雑な操作を必要とすることなく､定期的に受信する管理レポートにより社内ネットワークのセキュリティ状態を把握できます。また、お客様の既存ネットワークを再構築することなく設置が可能です。

迅速なサポートを可能にするリモート保守（無料）

万一の障害時にも、スピーディに問題解決を行います。
ネットワークに問題が発生した場合には、お客様よりアレクソンサポートセンターにお問い合わせください。お客様よりご了解を頂いた上で、ライセンス情報を元にUTMの設定確認や障害の切り分けを行います。

機能イメージ

UTM100は複数のネットワークセキュリティを1台にパッケージ化。
ユーザー様に運用・管理の負担が少ないシステムです。

ALEXON

セキュリティ × パフォーマンス = UTM100

UTM100 は、高度な脅威検出エンジンをバックボーンにしたセキュリティとハードウェアに最適化されたシステムで非常に優れたパフォーマンスを実現しています。
高度な攻撃や脅威の阻止に必要な機能を搭載し、信頼できるユーザーに対しては安全なネットワークアクセスを提供します。

ネットワーク防御

ファイアウォール

ファイアウォールは、社内ネットワークとインターネットの間で決められたルールの下、出入りするデータを監視し、データの通過・破棄を行います。
UTM100は、あらかじめ決められているルールを基にネットワークを保護し、セキュリティを高めます。

フィッシングサイト防御

インターネット上には偽装サイトが氾濫しており、アクセス元のパソコン内の情報の収集が行われております。
UTM100は、そういった偽装サイトをデータベースを参照して見破り、アクセスをさせない様にします。

Webウイルス防御

ウイルス感染はメールだけではなく、ウイルスを仕込まれたサイトにアクセスするだけで感染する場合があります。
UTM100は、そういったウイルスサイトを保持した情報で見破り、アクセスをさせない様にします。

侵入検知･防御

インターネット環境から、社内ネットワークに通過してきた通信をモニタしています。ファイアウォールだけでは阻止できない高度な攻撃や不正侵入･攻撃、またその兆候をもった通信を検知し、外部への情報流出を防御します。UTM100は、パフォーマンスを最適化したIPS(侵入防御システム)とDoS攻撃防止機能により、外的攻撃からシステムを保護します。

ウイルスメール防御

ウイルスメールは、UTM100上でブロックし、機密データの安全性を確保します。パソコンには、ウイルスメールをブロックした旨をメールで通知します。

SPAMメール防御(Proのみ)

最新の解析情報をリアルタイムに利用し、新種･未知のスパムを検出。個人情報の窃取、銀行口座詐欺、フィッシング詐欺などの最新の攻撃からユーザーを保護します。

URLフィルタリング

業務には不要な特定のサイトへのアクセスをブロックし、業務効率向上を図ることができます。データベースに含まれる109種類のカテゴリの3,500万件以上のサイトを活用して、不適切なコンテンツの閲覧などに関する法的な問題への懸念を排除しながら生産性を大きく向上します。

スパイウェア防御

スパイウェアとは、パソコンにインストールされたアプリケーションから特定の場所に対して、情報を発信するものです。
UTM100は、外部から送られてくるスパイウェアに感染するのを防御するだけではなく、LAN内のパソコンからの通信を監視し、スパイウェアによる通信を遮断します。

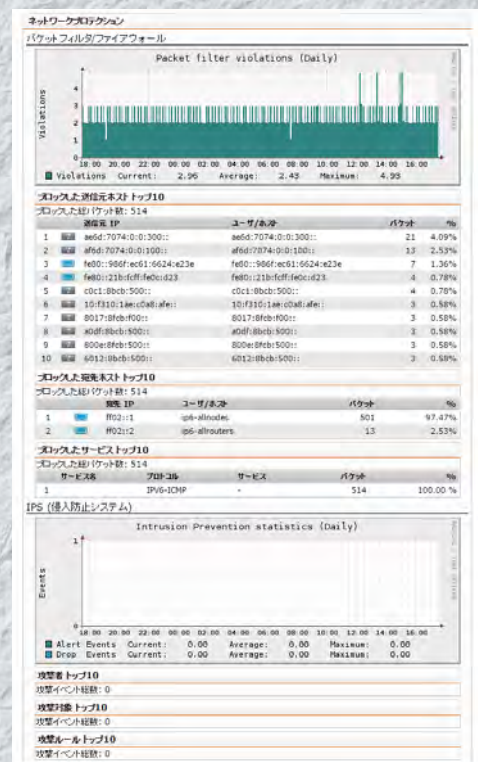
P2Pアプリケーション制御

P2Pとは、インターネットを介して一対一で通信を行い、データや画像を送受信する事ができるソフトウェアで、情報漏えいの温床となります。
UTM100は、LAN内のパソコンからの通信を監視し、該当の通信を遮断します。

メッセンジャー制御

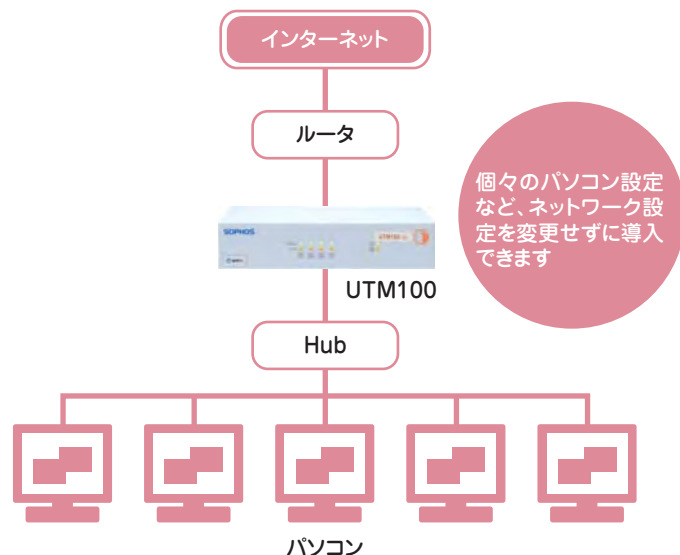
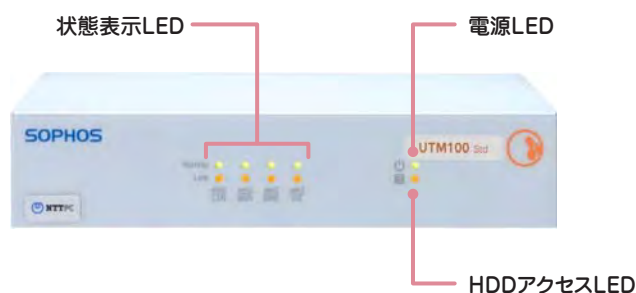
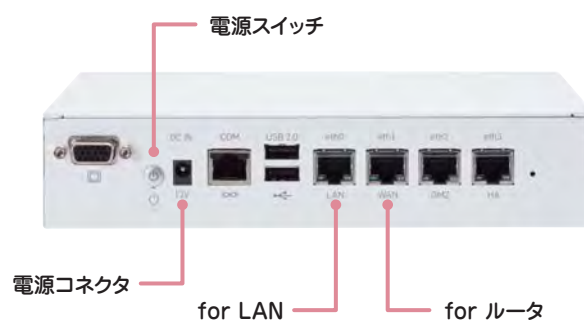
メッセンジャーとは、インターネットを介して特定の相手とメッセージや添付ファイルを送る事ができるソフトウェアで、情報漏えいの温床となります。
UTM100は、指定したメッセンジャーの通信を遮断します。

管理レポート

ひと目でネットワークの利用状況が把握できるグラフ形式のレポートでユーザーの状況を正確に把握できます。

管理レポート(一部抜粋)

UTM100 各機種の主要機能

	UTM100 Std S	UTM100 Std M	UTM100 Std L	UTM100 Pro S	UTM100 Pro M	UTM100 Pro L
Firewall 送受信時データチェック	●	●	●	●	●	●
IPS / IDS 不正侵入検知・防御	●	●	●	●	●	●
Application Control アプリケーション制御	●	●	●	●	●	●
URL Filtering アクセス URL 制限	●	●	●	●	●	●
Anti WEB Virus Web ウイルス防御	●	●	●	●	●	●
Anti Mail Virus ウイルスメール防御	●	●	●	●	●	●
Anti Spam スパムメール防御				●	●	●
Client 保護クライアント数	推奨 20	推奨 20	推奨 20	推奨 40	推奨 40	推奨 40
License ライセンス期間	5年	6年	7年	5年	6年	7年

接続構成例

前面

背面

仕様概要

		UTM100	
		Std	Pro
セキュリティ	保護クライアント数	推奨 20ユーザー	推奨 40ユーザー
	通信プロトコル	IPv4,IPv6	IPv4,IPv6
	ファイアウォール※1	●	●
	侵入検知·防御(IPS/IDS)※2	●	●
	ウイルスメール防御	●	●
	対応プロトコル	POP3	POP3
	Webウイルス防御	●	●
	対応プロトコル	FTP※2,HTTP	FTP※2,HTTP
	フィッシングサイト防御	●	●
	URLフィルタリング※1	●	●
	ブロック対象	カテゴリ、指定アドレス	カテゴリ、指定アドレス
	スパイウェア防御	●	●
	P2Pアプリケーション制御※1	●	●
	メッセンジャー制御※1	●	●
	スパムメール制御	-	●

		UTM100
		Std / Pro
ハードウェア仕様	ハードディスク容量	320GB
	主記憶(RAM)容量	2GB
	LANインターフェース	10/100/1000Base TX ×4
	USBコネクタ	2ポート
	COMコネクタ	1ポート
	VGAコネクタ	1ポート
	外部電源	100-24V AC(専用ACアダプタ)
	周波数	50-60Hz
	消費電力	最大21.6W
	ハードウェア形態	ゲートウェイ型
	外形寸法	210(W)×145(D)×44(H)mm(突起物を除く)
	質量	約1.15kg
	使用環境	温度0~40℃、湿度10~90%(但し結露なきこと)
	取得認定	VCCI ClassB、PSE、CB、CE、FCC ClassB、C-Tick、UL、CCC

安全上のご注意

●正しく安全にお使いいただくために、ご使用の前には「取扱説明書」をよくお読みください。
●水、湿気、ほこり、油煙等の多い場所や密閉された状態で設置しないでください。火災、感電、故障等の原因となることがあります。

●本製品は機器構成によっては接続出来ない場合がありますので、あらかじめご了承ください。●本製品を医療機器の近くでは使用しないでください。●本資料は2015年1月現在のものです。仕様および内容は予告なく変更する場合があります。● 内蔵のハードディスクドライブは保守対象部品です。ご使用状態により、交換が必要になる場合があります。●本製品の故障・誤動作・不具合あるいは停電等の外部要因によって異常な動作が発生した場合や、異常動作の発生により生じた損害等の純正経済損失につきましては、一切その責任を負いかねますので、あらかじめご了承ください。
※1 ユーザー様毎の設定が必要になります。※2 初期値無効です。

bfh3.UTM

輸入元
株式会社エヌ・ティ・ティ ピー・シー コミュニケーションズ

販売元

株式会社 アレクソン

ビジネスパートナー部 第一営業グループ
〒103-0013 東京都中央区日本橋人形町2-25-13 リンレイ日本橋ビル5F
TEL 03-3667-2276 FAX 03-3667-5329 IP-Phone 050-5501-9711

ビジネスパートナー部 第二営業グループ
〒664-0026 兵庫県伊丹市寺本3-207-1
TEL 072-777-1584 FAX 072-780-2060 IP-Phone 050-5507-5125

ビジネスパートナー部 第三営業グループ
〒819-0025 福岡県福岡市西区石丸2丁目40番8号
TEL 092-477-3677 FAX 092-477-3678
ホームページ http://www.alexon.co.jp/